On the implementation of the DME-KEM cryptosystem

Martin, Michel, Ignacio

December 16, 2017

Abstract

This document describes the exact version of the DME-KEM cryptosystem (developed by Ignacio Luengo) that is provided by our implementation.

1 DME-KEM cryptosystem

The DME-KEM cryptosystem is based on a polynomial map

$$P : (\mathbb{F}_q)^{nm} \to (\mathbb{F}_q)^{nm}$$

where $\mathbb{F}_q$ is the finite field of $q = 2^e$ elements and $2 \leq n < m$ are fixed integers. The map P is the composition of three $\mathbb{F}_q$-linear maps $L_1, L_2, L_3 : (\mathbb{F}_q)^{nm} \to (\mathbb{F}_q)^{nm}$, two exponential maps $G_1 : (\mathbb{F}_{q^n})^m \to (\mathbb{F}_{q^n})^m$ and $G_2 : (\mathbb{F}_{q^m})^n \to (\mathbb{F}_{q^m})^n$, two isomorphisms $J_n : (\mathbb{F}_q)^{nm} \to (\mathbb{F}_{q^n})^m$ and $J_m : (\mathbb{F}_q)^{nm} \to (\mathbb{F}_{q^m})^n$, and a permutation map $P_{n,m} : (\mathbb{F}_q)^{nm} \to (\mathbb{F}_q)^{nm}$.

$$P = L_3 \circ J_m^{-1} \circ G_2 \circ J_m \circ L_2 \circ P_{n,m} \circ J_n^{-1} \circ G_1 \circ J_n \circ L_1 \tag{1}$$

The maps $G_1, G_2, J_n, J_m, P_{n,m}$ are fixed. The secret key consists of the other three maps L_1, L_2, L_3, which are chosen to be invertible. Anyone in possesion of the secret key will be able to compute $P^{-1}(c)$ for any $c \in (\mathbb{F}_q)^{nm}$, since the individual maps that define P are easily inverted. The public key consists of the nm polynomials in nm variables that define P. Of course, anyone with the public key is able to compute $P(x)$ for $x \in (\mathbb{F}_q)^{nm}$. The security of the cryptosystem relies on the (so far unproven) conjecture that it is very hard to recover the maps L_1, L_2, L_3 from the polynomial expression of P, and that it is hard to compute $P^{-1}(c)$ for a given $c \in (\mathbb{F}_q)^{nm}$ without access to L_1, L_2, L_3.

The map $G_1 : (\mathbb{F}_{q^n})^m \to (\mathbb{F}_{q^n})^m$ is of the form

$$G_1(u_1, \ldots, u_m) = (u_1^{a_{11}} \cdots u_m^{a_{1m}}, \ldots, u_1^{a_{m1}} \cdots u_m^{a_{mm}})$$

where the exponent matrix $A = (a_{ij}) \in \mathbb{Z}^{m \times m}$ is invertible modulo $q^n - 1$ and the entries a_{ij} are either zero or powers of two (up to q^{n-1}). The invertibility condition is equivalent to $\gcd(det(A), q^n - 1) = 1$, and implies that $G_1 : (\mathbb{F}_{q^n}^*)^m \to (\mathbb{F}_{q^n}^*)^m$ is a bijection whose inverse $G_1^{-1} : (\mathbb{F}_{q^n}^*)^m \to (\mathbb{F}_{q^n}^*)^m$ is also an exponential map, defined by an exponent matrix $A' \in \mathbb{Z}^{m \times m}$ such that $AA' \equiv I \pmod{q^n - 1}$. Similarly, the map $G_2 : (\mathbb{F}_{q^m})^n \to (\mathbb{F}_{q^m})^n$ is of the form

$$G_2(w_1, \ldots, w_n) = (w_1^{b_{11}} \cdots w_n^{b_{1n}}, \ldots, w_1^{b_{n1}} \cdots w_n^{b_{nn}})$$

where the exponent matrix $B = (b_{ij}) \in \mathbb{Z}^{n \times n}$ is invertible modulo $q^m - 1$ and the entries b_{ij} are either zero or powers of two (up to q^{m-1}). This implies that $G_2 : (\mathbb{F}_{q^m}^*)^n \to (\mathbb{F}_{q^m}^*)^n$ is a bijection whose inverse is the exponential map G_2^{-1} defined by the exponent matrix $B' \in \mathbb{Z}^{n \times n}$ such that $BB' \equiv I$

(mod $q^m - 1$). The entries of the matrices A' and B', which can be taken as non-negative integers bounded above by $q^n - 1$ and $q^m - 1$, respectively, are not necessarily powers of two or zero (and they are usually not). Part of the security of the cryptosystem is conjectured to come from the fact that the entries of A' and B' have many non-zero bits.

The isomorphism $J_n : (\mathbb{F}_q)^{nm} \to (\mathbb{F}_{q^n})^m$ of $\mathbb{F}_q$-vector spaces, is actually made of m copies of an isomorphism $K_n : (\mathbb{F}_q)^n \to \mathbb{F}_{q^n}$.

$$J_n(x_0, \dots, x_{nm-1}) = (K_n(x_0, \dots, x_{n-1}), \dots, K_n(x_{(m-1)n}, \dots, x_{nm-1})$$

The isomorphism $K_n : (\mathbb{F}_q)^n \to \mathbb{F}_{q^n}$ is defined by

$$K_n(x_0, \dots, x_{n-1}) = x_0 + x_1 T + \cdots + x_{n-1} T^{n-1}$$

where $\mathbb{F}_{q^n} = \mathbb{F}_q[T]$, i.e. T is a generator of the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$.

Similarly, the isomorphism $J_m : (\mathbb{F}_q)^{nm} \to (\mathbb{F}_{q^m})^n$ of $\mathbb{F}_q$-vector spaces, consists of n copies of an isomorphism $K_m : (\mathbb{F}_q)^m \to \mathbb{F}_{q^m}$.

$$J_m(x_0, \dots, x_{nm-1}) = (K_m(x_0, \dots, x_{m-1}), \dots, K_m(x_{(n-1)m}, \dots, x_{nm-1})$$

The isomorphism $K_m : (\mathbb{F}_q)^m \to \mathbb{F}_{q^m}$ is defined by

$$K_m(x_0, \dots, x_{m-1}) = x_0 + x_1 S + \cdots + x_{m-1} S^{m-1}$$

where $\mathbb{F}_{q^m} = \mathbb{F}_q[S]$, i.e. S is a generator of the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$.

A vector $v \in (\mathbb{F}_q)^{nm}$ can be decomposed as n vectors $v_{(1)}, \dots, v_{(n)} \in (\mathbb{F}_q)^m$, or as m vectors $v^{(1)}, \dots, v^{(m)} \in (\mathbb{F}_q)^n$, by splitting its coordinates in an orderly fashion. The permutation map $P_{n,m}$ is chosen in such a way that $w = P_{n,m}(v)$ and $v^{(1)} \neq 0, \dots, v^{(m)} \neq 0$ implies $w_{(1)} \neq 0, \dots, w_{(n)} \neq 0$. Such a map always exists since $n < m$.

The map L_1 has a block structure, in particular, m blocks of $n \times n$. More precisely, the first block acts on the first n variables $x_0, \dots, x_{n-1}$, the second block on $x_n, \dots, x_{2n-1}$, etc. The other two maps L_2, L_3 also have a block structure, but in this case n blocks of $m \times m$. This means that a secret key consists of $mn^2 + 2nm^2$ coefficients in $\mathbb{F}_q$.

It is easy to see that if $c = P(x)$ and $x^{(1)} \neq 0, \dots, x^{(m)} \neq 0$, then $c_{(1)} \neq 0, \dots, c_{(n)} \neq 0$. If we define

$$X = \Big\{x \in (\mathbb{F}_q)^{nm} \ : \ x^{(1)} \neq 0, \dots, x^{(m)} \neq 0\Big\}, \qquad C = \Big\{c \in (\mathbb{F}_q)^{nm} \ : \ c_{(1)} \neq 0, \dots, c_{(n)} \neq 0\Big\},$$

then $P(X) \subseteq C$. Moreover, for any $x \in X$, the vectors $(J_n \circ L_1)(x) \in (\mathbb{F}_{q^n})^m$ and $(J_m \circ L_2 \circ P_{n,m} \circ J_n^{-1} \circ G_1 \circ J_n \circ L_1)(x) \in (\mathbb{F}_{q^m})^n$ have all their entries different from zero. This means that for any $x \in X$, the exponential maps G_1 and G_2 in (1) receive vectors in the subdomain where they are invertible. For any $c \in P(X) \subset C$, we can compute $x = P^{-1}(c) \in X$ by inverting each of the maps in (1). Note that $|X| = (q^n - 1)^m < |C| = (q^m - 1)^n$, so there are elements in $c \in C$ such that $P^{-1}(c)$ is not well-defined.

The polynomial map $P(x) = (p_0(x), \dots, p_{nm-1}(x))$ has a very particular structure. Each of its component $p_i \in \mathbb{F}_q[x_0, \dots, x_{nm-1}]$ is a sparse polynomial (with a predictable number of terms depending on the exponential maps G_1, G_2, and the permutation $P_{n,m}$). Moreover, the first m polynomials $p_0, \dots, p_{m-1}$ share the same monomials (although with different coefficients), the second group of polynomials $p_m, \dots, p_{2m-1}$ also share monomials, etc. Of course, the coefficients depend on the secret key maps L_1, L_2, L_3. These coefficients constitute the public key. Clearly, anyone with those coefficients is able to compute $P(x)$ for any $x \in (\mathbb{F}_q)^{nm}$.

2 Implementation

We decided to implement the case $n = 2$, $m = 3$, $e = 48$. Of course, we need to specify which maps G_1, G_2, J_2, J_3, $P_{2,3}$ we are using. We chose G_1 and G_2 the exponential maps induced by

$$A = \begin{bmatrix} 2^{E_{11}} & 2^{E_{12}} & 0 \\ 2^{E_{21}} & 0 & 2^{E_{23}} \\ 0 & 2^{E_{32}} & 2^{E_{33}} \end{bmatrix} \qquad B = \begin{bmatrix} 2^{F_{11}} & 2^{F_{12}} \\ 2^{F_{21}} & 2^{F_{22}} \end{bmatrix}$$

where $0 \leq E_{11}, E_{12}, E_{21}, E_{23}, E_{32}, E_{33} < 96$ and $0 \leq F_{11}, F_{12}, F_{21}, F_{22} < 144$ were chosen in such a way that $\gcd(\det(A), 2^{96} - 1) = 1$ and $\gcd(\det(B), 2^{144} - 1) = 1$, and that the modular inverses A' and B' of A and B (modulo $2^{96} - 1$ and $2^{144} - 1$, respectively) have the maximum total number of non-zero bits. This resulted in $E_{11} = 24, E_{12} = 59, E_{21} = 21, E_{23} = 28, E_{32} = 29, E_{33} = 65$ and $F_{11} = 50, F_{12} = 24, F_{21} = 7, F_{22} = 88$.

The map $P_{2,3}$ was chosen to be the identity map. The maps J_2 and J_3 are induced by the maps K_2 and K_3, which depend only on the choice of elements $T \in \mathbb{F}_{q^2}$ and $S \in \mathbb{F}_{q^3}$ such that $\mathbb{F}_{q^2} = \mathbb{F}_q[T]$ and $\mathbb{F}_{q^3} = \mathbb{F}_q[S]$. This is equivalent to find irreducible polynomials $f_2(T) = T^2 + aT + b$ and $f_3(S) = S^3 + cS^2 + dS + e$ over $\mathbb{F}_q$, and define the fields $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^3}$ as $\mathbb{F}_q[T]/\langle f_2 \rangle$ and $\mathbb{F}_q[S]/\langle f_3 \rangle$. We decided to use $\mathbb{F}_q = \mathbb{F}_2[t]/\langle t^{48} + t^{28} + t^{27} + t + 1 \rangle$, and to choose $a, b, c, d, e \in \mathbb{F}_q$ randomly (until irreducible f_2 and f_3 were found).

$$a = 1 + t + t^3 + t^4 + t^8 + t^9 + t^{13} + t^{19} + t^{20} + t^{21} + t^{22} + t^{23} + t^{24} + t^{25} + t^{26} + t^{29} + t^{34} + t^{36} + t^{38} + t^{43}$$

$$\begin{aligned} b = 1 &+ t^2 + t^3 + t^7 + t^8 + t^9 + t^{14} + t^{16} + t^{17} + t^{18} + t^{21} + t^{22} + t^{23} + t^{24} + t^{26} + t^{27} + t^{30} + t^{31} + t^{35} \\ &+ t^{37} + t^{38} + t^{39} + t^{40} + t^{43} + t^{45} + t^{46} + t^{47} \end{aligned}$$

$$\begin{aligned} c = t &+ t^2 + t^3 + t^5 + t^8 + t^{11} + t^{12} + t^{13} + t^{14} + t^{15} + t^{17} + t^{19} + t^{20} + t^{22} + t^{24} + t^{26} + t^{29} + t^{30} \\ &+ t^{32} + t^{33} + t^{34} + t^{36} + t^{37} + t^{38} + t^{39} \end{aligned}$$

$$\begin{aligned} d = 1 + t &+ t^2 + t^3 + t^4 + t^7 + t^8 + t^8 + t^{10} + t^{12} + t^{14} + t^{15} + t^{16} + t^{17} + t^{20} + t^{21} + t^{25} + t^{30} + t^{31} \\ &+ t^{32} + t^{33} + t^{37} + t^{38} + t^{41} + t^{44} + t^{45} + t^{46} \end{aligned}$$

$$\begin{aligned} e = t &+ t^2 + t^5 + t^6 + t^8 + t^9 + t^{11} + t^{12} + t^{13} + t^{14} + t^{15} + t^{17} + t^{19} + t^{20} + t^{23} + t^{24} + t^{25} + t^{26} + t^{32} \\ &+ t^{35} + t^{38} + t^{39} + t^{42} + t^{46} + t^{47} \end{aligned}$$

The serialization of elements of $\mathbb{F}_q$, i.e. the map the allow us to write elements of $\mathbb{F}_q$ as sequence of bytes, is defined as follows: first, write the element as a reduced polynomial modulo $t^{48} + t^{28} + t^{27} + t + 1$, then map this degree 47 polynomial to an integer by substituting $t = 2$, then write the resulting integer in base 256, and finally output the six digits starting with the most significative. Serialization of vectors in $(\mathbb{F}_q)^6$ apply the serialization described above to the first coordinate, then to the second, etc. Serialization of secret keys and public keys is done by serializing the coefficients of L_1, L_2, L_3 or the coefficients of $p_0, \ldots, p_5$. The specific order in which this is done is made clear in the source code (and clearly irrelevant once it has been fixed).

The KEM primitives are implemented on top of what we have described so far. Keypair generation is done by randomly choosing the coefficients of the matrices L_1, L_2, L_3 and computing the corresponding coefficients of $p_0, \ldots, p_5$ by interpolation at some precomputed vectors.

The second primitive creates a shared secret of 33 bytes, then interleaves a byte 0x01 between the $11th$ and $12th$, another 0x01 between the $22nd$ and $23rd$, and another 0x01 at the end of the sequence. This gives a new sequence of 36 bytes, which corresponds (after deserialization) to a vector $x \in X \subset (\mathbb{F}_q)^6$. The ciphertext is the serialization of $P(x)$, which is a sequence of bytes of length 36. Clearly, this can be done by anyone possessing the public key.

Finally, the last primitive recovers the shared secret using the secret key, by computing P^{-1} of the deserialization of the ciphertext, and removing the extra bytes (which are verified to match 0x01).

With all the parameters as described above, we have secret keys of 288 bytes, public keys of 2304 bytes, shared secrets of 33 bytes, and ciphertexts of 36 bytes.